

March 13, 2013

HIPAA Omnibus Rule's Impact on Notices of Privacy Practices

RESOURCE LINKS

[Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules](#)

Published January 25, 2013

This health reform alert summarizes the key changes to the Notice of Privacy Practices (“NPP”)¹ requirements in the revised Health Insurance Portability and Accountability Act (“HIPAA”) regulations (the “Omnibus Rule”)² as well as what covered entities need to do to be compliant.³ Because many covered entities may have modified their NPPs based on the Notice of Proposed Rulemaking issued on July 14, 2010 (“NPRM”),⁴ this alert also details the similarities and differences between the NPRM and the Omnibus Rule related to NPPs. In addition, Table 1 of this alert provides a quick summary of the NPRM proposals adopted—or not adopted—by the Omnibus Rule.

As covered entities work toward compliance, they should keep in mind that the Omnibus Rule becomes effective on March 26, 2013, but the deadline for compliance is **September 23, 2013**.

¹ Under 45 C.F.R. § 164.520, most covered entities must have and distribute a NPP describing (1) the uses and disclosures of protected health information that a covered entity may make, (2) the covered entity’s legal duties and privacy practices with respect to protected health information, and (3) the individual’s rights concerning protected health information.

² Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Department of Health and Human Services, Office of the Secretary (45 C.F.R. Parts 160 and 164), 78 Fed. Reg. 5566 (Jan. 25, 2013).

³ For information on the Omnibus Rule’s other requirements, see the following Epstein Becker Green health reform alerts: *Overview of Modifications to the HIPAA Privacy, Security, and Enforcement Rules*, Jan. 20, 2013, <http://www.ebglaw.com/showclientalert.aspx?Show=16954>; *Four Key Areas of the New HIPAA Privacy Regulations*, Feb. 1, 2013, <http://www.ebglaw.com/showclientalert.aspx?Show=17013>; and *Key Compliance Actions for the New HIPAA Privacy Regulations*, Feb. 19, 2013, <http://www.ebglaw.com/showclientalert.aspx?Show=17053>.

⁴ 75 Fed. Reg. 40868 (July 14, 2010).

Key Changes to NPP Content

1. Description of Uses and Disclosures Requiring Authorization

In the NPRM, the U.S. Department of Health and Human Services (“HHS”) proposed amending 45 C.F.R. § 164.520(b)(1)(ii)(E) of the HIPAA Privacy Rule to require that NPPs include information regarding certain types of uses and disclosures of protected health information (“PHI”) that require an authorization under Sections 164.508(a)(2) through (a)(4). These include (1) most uses and disclosures of psychotherapy notes, (2) uses and disclosures of PHI for marketing purposes, and (3) disclosures that constitute a sale of PHI. The NPRM also proposed requiring that a NPP contain a statement that other uses and disclosures not described in the NPP will be made only with an individual’s authorization.

The Omnibus Rule finalizes the proposed modifications in full. Furthermore, the preamble of the Omnibus Rule (the “Preamble”) provides several clarifications in response to comments to the NPRM. First, the Preamble clarifies that a NPP need not list all situations regarding authorization. Second, a NPP does not need to include a description of a covered entity’s recordkeeping practices with respect to psychotherapy notes. Third, covered entities that do not record or maintain psychotherapy notes are not required to include a statement about the authorization requirement for uses and disclosures of psychotherapy notes.

2. Separate Statements for Certain Uses and Disclosures

The NPRM proposed modifying 45 C.F.R. § 164.520(b)(1)(iii), which requires a covered entity to include in its NPP separate statements about certain activities if the covered entity intends to engage in any of those activities. First, the NPRM proposed requiring a health care provider that has received financial remuneration for sending individuals treatment communications to notify individuals, through its NPP, of its intent to send these communications. Moreover, the NPRM proposed that covered entities would also be required to notify individuals of their right to opt out of receiving such communications. The Omnibus Rule does not adopt these requirements regarding treatment communications. Since the Omnibus Rule treats subsidized treatment communications as marketing communications (with some exceptions), covered entities will not be required to include a statement in their NPPs about such communications and an individual’s ability to opt out.

Second, the NPRM also proposed that a covered entity intending to contact an individual to raise funds must inform the individual of its intention and the individual’s right to opt out of receiving such communications. The Omnibus Rule adopts these requirements pertaining to fundraising communications. However, it should be noted that, with regard to such communications, a NPP is not required to include the mechanism for individuals to opt out.

Third, pursuant to both HIPAA and the Genetic Information Nondiscrimination Act,⁵ HHS published a separate notice of proposed rulemaking on October 7, 2009. This proposed rule required health plans intending to use or disclose PHI for underwriting purposes to include a statement in their NPPs that they are prohibited from using or disclosing an individual’s

⁵ 42 U.S.C. 2000ff, *et seq.*

genetic information for such purposes. The Omnibus Rule adopts this requirement but exempts long-term care policy issuers.⁶

3. Enhanced Patient Rights

The NPRM proposed to amend 45 C.F.R. § 164.520(b)(1)(iv)(A) to require inclusion of a statement in NPPs explaining that the covered entity must agree to a request to restrict disclosure of PHI to a health plan if the disclosure is for payment or health care operations and pertains to a health care item or service for which the individual has paid out of pocket in full. The Omnibus Rule adopts this proposal, but the Preamble clarifies that the requirement applies only to health care providers. The Preamble also notes that other types of covered entities may keep existing language specifying that they are not required to agree to a requested restriction.⁷

The Omnibus Rule also requires that covered entities revise their NPPs to address other modifications made to an individual's rights, including, but not limited to, the right to receive electronic copies of health information.⁸

4. Breach Notification Obligations

With regard to new breach notification obligations under Subpart D of Part 164, the NPRM requested comment on whether the Privacy Rule should require a specific statement regarding this new legal duty.

The Omnibus Rule requires covered entities to include in their NPPs a statement of affected individuals' notification rights after a breach of unsecured PHI. The Preamble clarifies that a covered entity will meet this requirement by including a simple statement that an individual has a right to, or will receive, notifications of breaches of his or her unsecured PHI. However, the Omnibus Rule does not prescribe the specific contents of such a statement, and the Preamble notes that the statement does not have to be entity-specific or describe the types of information to be provided in the breach notification.⁹

5. Appointment Reminders and Alternatives

Interestingly, the Omnibus Rule removes the requirement that a NPP include a statement that the covered entity may contact the individual to provide appointment reminders or information about treatment alternatives or other benefits and services that may be of interest to the individual.¹⁰ After March 26, 2013, covered entities will no longer be required to include this statement in their NPPs, but may continue to do so if they wish.

⁶ 45 C.F.R. § 164.520(b)(1)(iii)(C).

⁷ 78 Fed. Reg. 5566, 5624. See also 45 C.F.R. § 164.522(a)(1)(ii).

⁸ See 45 C.F.R. § 164.520(b)(1)(iv)(C); 45 C.F.R. § 164.524(c)(2)(ii).

⁹ 78 Fed. Reg. 5566, 5624-25.

¹⁰ 45 C.F.R. § 164.508(a)(3).

Posting and Distribution

Under the Privacy Rule, whenever there is a material change to a NPP, a covered entity must promptly revise and distribute its NPP. The Omnibus Rule confirms that the required amendments constitute material changes necessitating revision and redistribution of NPPs. Further, the Omnibus Rule provides for certain distribution requirements based on the type of covered entity.

A health plan that currently posts its NPP on its website must (1) prominently post the change or its revised NPP on its website by September 23, 2013 (the compliance date), and (2) provide the revised NPP, or information about the material change and how to obtain the revised NPP, in its next annual mailing to individuals then covered by the plan.¹¹ Health plans that do not have customer service websites must provide the revised NPP, or information about the material change and how to obtain the revised NPP, to individuals covered by the plan within 60 days of the material revision.¹²

The Omnibus Rule does not modify current requirements for health care providers to distribute NPP revisions.¹³ Therefore, when a health care provider with a direct treatment relationship with an individual revises its NPP, the provider must make the NPP available upon request on or after the effective date of the revision.¹⁴ Moreover, the provider must make the NPP available at the service delivery site and post the NPP in a clear and prominent location.¹⁵ The Preamble clarifies that a health care provider is required to give a copy of its NPP only to new patients—and not all individuals seeking treatment.¹⁶

Impact of Noncompliance by September 23, 2013

Noncompliance with the new NPP requirements could subject covered entities to government investigations, increased civil monetary penalties, resolution agreements, and complaints from patients and beneficiaries. As the Omnibus Rule affects individual rights, covered entities should be cognizant that failure to comply with the NPP requirements may be highly visible by patients and beneficiaries and can result in greater scrutiny by the HHS Office of Civil Rights, the agency with enforcement authority under HIPAA. Therefore, covered entities should make sure to evaluate the content and distribution practices of their NPPs and determine if any changes are necessary to comply with the Omnibus Rule.

¹¹ 45 C.F.R. § 164.520(c)(1)(v)(A).

¹² 45 C.F.R. § 164.520(c)(1)(v)(B).

¹³ 78 Fed. Reg. 5566, 5625.

¹⁴ *Id.*

¹⁵ *Id.*

¹⁶ *Id.*

Table 1 – Summary of Key Changes to NPP Requirements: Which NPRM Proposals Were Adopted (or Not Adopted) by the Omnibus Rule?

NPRM	Omnibus Rule
<p>Uses and Disclosures of PHI Requiring Authorization – NPPs must include information regarding certain types of uses and disclosures of PHI that require an authorization.</p>	<p>Adopted.</p>
<p>Treatment Communications – A health care provider that has received financial remuneration for sending individuals treatment communications must notify individuals, through its NPP, of its intent to send these communications. Covered entities must notify individuals of their right to opt out of receiving such communications.</p>	<p>Not adopted.</p>
<p>Fundraising – A covered entity that intends to contact an individual to raise funds must inform the individual of its intention and the individual’s right to opt out of receiving such communications.</p>	<p>Adopted.</p>
<p>Use or Disclose of PHI for Underwriting Purposes – Health plans intending to use or disclose PHI for underwriting purposes must include a statement in their NPPs that they are prohibited from using or disclosing PHI that is an individual’s genetic information for such purposes.</p>	<p>Adopted, but long-term care policy issuers are exempted.</p>
<p>Restrictions on Disclosure of PHI to Health Plan – NPPs must have a statement explaining that the covered entity must agree to a request to restrict disclosure of PHI to a health plan if the disclosure is for payment or health care operations and pertains to a health care item or service for which the individual has paid out of pocket in full.</p>	<p>Adopted.</p>
<p>Breach Notification Obligations – The NPRM requested comment on whether the Privacy Rule should require a specific statement regarding new breach notification obligations.</p>	<p>Covered entities must include a statement of affected individuals’ notification rights after a breach of unsecured PHI.</p>
<p>Appointment Reminders – NPPs must include a statement that the covered entity may contact the individual to provide appointment reminders or information about alternatives.</p>	<p>Not adopted.</p>

For more information about this issue of *IMPLEMENTING HEALTH AND INSURANCE REFORM*, please contact one of the authors below or the member of the firm who normally handles your legal matters.

[Patricia M. Wagner](#)

Member of the Firm
Epstein Becker Green
Washington, D.C.
(202) 861-4182
PWagner@ebglaw.com

[Brandon C. Ge](#)

Associate
Epstein Becker Green
Washington, D.C.
(202) 861-1841
BGe@ebglaw.com

[Alaap B. Shah](#)

Associate
Epstein Becker Green
Washington, D.C.
(202) 861-1877
ABShah@ebglaw.com

Information published in *IMPLEMENTING HEALTH AND INSURANCE REFORM* is not intended to be, nor should it be considered, legal advice. Readers should consult an attorney to discuss specific situations in further detail.